ISSN 2277-2685
IJESR/April-June. 2026/ Vol-16/Issue-2/109-114
Voora Pooja *et. al.*, / International Journal of Engineering & Science Research
Full Length Article

Smart Key Management System

Dr N Pradeep Kumar Goud[1], Voora Pooja[2], Tulasi Srujana[3], Pallapu Venkata Jyothirmayee[4]
[1]Assistant Professor; Department Of Electronics And Communication Engineering Bhoj Reddy Engineering College For Women Hyderabad India.
[2,3,4]B.Tech Students; Department Of Electronics And Communication Engineering Bhoj Reddy Engineering College For Women Hyderabad India.
Mail Id; voorepooja09@gmail.com[2],tulasisrujana2004@gmail.com[3] ,pallapujyothi49@gmail.com[4]
Accepted 05-04-2026

Abstract
Efficient control of physical keys remains a major security concern in offices, banks, industries, laboratories, and educational institutions. Conventional key handling methods generally depend on manual registers, lockers, or supervision, which often result in poor accountability, misplaced keys, unauthorized access, and operational delays. To address these challenges, this paper presents a Smart Key Management System based on biometric authentication and embedded automation. The proposed system uses an ESP32 microcontroller integrated with an R307 fingerprint sensor, servo motor, liquid crystal display (LCD), LEDs, and a buzzer. Access to stored keys is granted only after successful fingerprint verification, ensuring that only registered users can retrieve authorized keys. The servo motor automatically unlocks the assigned key slot, while failed authentication attempts activate warning alerts. In addition, the system can maintain digital logs of user access activity, improving transparency and monitoring. The prototype is developed using Embedded C/C++ in the Arduino IDE environment. Experimental evaluation indicates that the system enhances security, reduces human intervention, minimizes errors, and provides a scalable framework for future Internet of Things (IoT) integration. The proposed model offers a practical and cost-effective solution for modern key management applications.
Keywords
Smart Key Management, ESP32, Fingerprint Authentication, Embedded Systems, Access Control, Security Automation

Introduction

Physical key management is a critical but frequently neglected aspect of organizational security. Many institutions continue to use conventional methods such as lock cabinets, paper registers, and manual supervision for issuing and returning keys. Although these methods are simple to implement, they often suffer from poor traceability, delayed access, missing keys, and unauthorized usage. In sensitive environments such as banks, laboratories, server rooms, and industrial facilities, these weaknesses can create serious security risks.

Recent developments in embedded systems and biometric technologies have enabled more secure alternatives for access management. Fingerprint authentication is one of the most reliable biometric techniques because fingerprints are unique, difficult to duplicate, and convenient for users. Integrating fingerprint recognition with automated locking systems can significantly improve security while reducing dependence on manual monitoring.

This paper proposes a Smart Key Management System that combines biometric verification with real-time automation. The system uses an ESP32 microcontroller as the central controller, which communicates with a fingerprint sensor, display unit, and locking mechanism. Once an authorized fingerprint is recognized, the system releases the corresponding key slot through a servo motor. Unauthorized attempts trigger alarms and deny access. The solution is intended to improve security, accountability, and operational efficiency in organizations requiring controlled key usage.

Problem Statement

Traditional key management systems present several operational and security limitations. Keys are often handled manually without identity verification, making unauthorized borrowing possible. Register-based systems depend heavily on human discipline and may contain incomplete or inaccurate records. In some cases, keys are misplaced or duplicated without detection. These problems highlight the need for an intelligent system capable of authenticating users, automating key release, and maintaining accurate access logs.

Authentication and Verification

Authentication and verification form the foundation of the Smart Key Management System, as they determine whether a user is permitted to access secured keys. In conventional key storage methods, verification is generally carried out manually through supervisors, written registers, or physical observation. Such practices are often slow, inconsistent, and vulnerable to unauthorized use. To overcome these limitations, the proposed system applies biometric authentication using fingerprint recognition.

The fingerprint sensor captures the biometric pattern of the user and transmits the data to the ESP32 microcontroller for processing. The controller compares the captured fingerprint with templates stored in the internal database. If a valid match is found, the system grants access to the assigned key compartment. If the fingerprint does not match, the request is rejected immediately.

This automated method improves reliability and reduces dependence on human supervision. Since fingerprints are unique to each person, biometric verification offers stronger protection than passwords, ID cards, or manual registers. The system also operates in real time, allowing fast responses and convenient access. As a result, authentication becomes the first and most important security layer of the Smart Key Management System.

Fingerprint-Based Authentication System

The Smart Key Management System uses the R307 fingerprint sensor as the primary biometric device. Fingerprints are considered highly reliable because ridge patterns differ from one person to another, even among twins. This uniqueness makes fingerprints suitable for secure identity verification.

During operation, the user places a finger on the sensor surface. The sensor captures the image and converts it into a digital template. This template is transmitted to the ESP32 microcontroller, which compares it with enrolled fingerprint records stored in memory. If a matching template is identified, the user is authenticated successfully. Otherwise, access is denied.

The R307 sensor can store multiple templates, allowing the system to support several users. Its fast recognition speed helps reduce waiting time, while accurate matching improves user experience. Because fingerprints are difficult to replicate, the method provides stronger security than ordinary lock-and-key arrangements.

Accessing the Keys

After successful authentication, the Smart Key Management System proceeds to the key access stage. This phase is responsible for allowing an authorized user to retrieve the required key in a secure and controlled manner. While authentication confirms the identity of the user, the access mechanism ensures that only validated users can physically interact with the stored keys.

The process is managed by the ESP32 microcontroller, which controls connected hardware devices such as the servo motor, LEDs, buzzer, and LCD display. Once authentication is confirmed, the controller activates the unlocking mechanism automatically without the need for manual supervision.

Automated key access offers several advantages over conventional methods. It reduces delays, minimizes human error, improves operational efficiency, and enhances overall security. Since the system performs all actions electronically, the chances of unauthorized handling are greatly reduced. This chapter explains how the key access system functions, the role of each component, and the security measures involved.

Key Access Mechanism

Once a user is authenticated successfully, the controller initiates the key release process. The ESP32 sends a control signal to the servo motor connected to the designated key compartment. The motor rotates to a predefined angle, unlocking the slot and allowing the user to retrieve the assigned key.

After a fixed interval, the servo motor returns to its original position and locks the compartment again. This automatic re-locking feature ensures that the key slot is not left open unnecessarily.

The complete mechanism operates quickly and efficiently. It guarantees that access is granted only after proper verification and helps prevent misuse. By replacing manual handling with automation, the system increases reliability and provides a better user experience.

Block Diagram of Key Access System

The key access system is designed around the ESP32 microcontroller, which functions as the main control unit. It receives authentication results from the fingerprint sensor and processes the decision logic. If access is approved, the controller sends commands to the servo motor for unlocking the key slot.

At the same time, the LCD displays status messages such as “Access Granted” or operational instructions. LEDs provide visual indicators, while the buzzer generates alerts during denied attempts or system warnings.

The structured communication between input devices, controller, and output modules ensures smooth operation. Block diagrams are valuable in representing this interaction because they simplify the system architecture and help during development, maintenance, and troubleshooting.

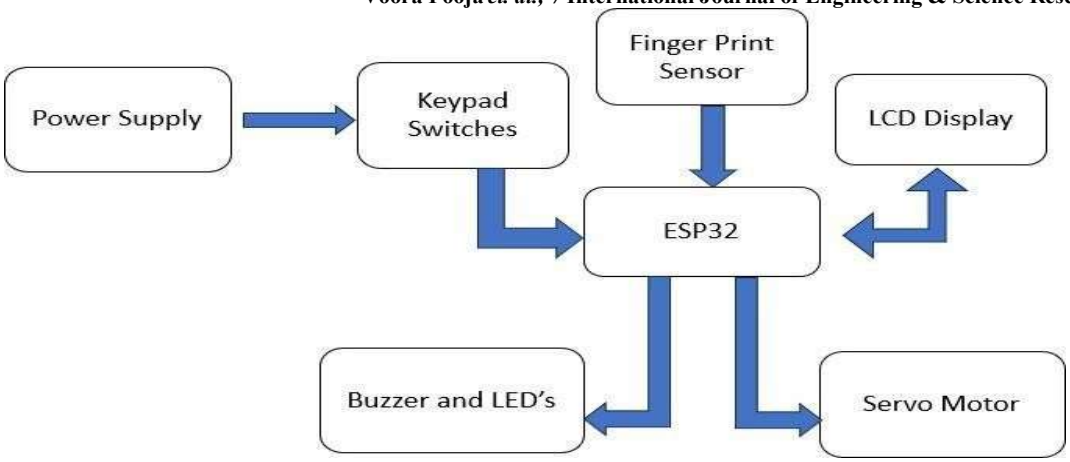

Fig 1; Block Diagram

Working of Servo Motor Control

The servo motor is the primary mechanical component responsible for locking and unlocking the key compartment. It operates according to pulse-width modulation (PWM) signals generated by the ESP32.

When the user is authenticated, the controller sends a signal that rotates the servo shaft to a specified angle, opening the lock. After a programmed delay, the controller commands the servo to rotate back to its original position, restoring the locked state.

Servo motors are preferred in such applications because they offer precise angular movement, low power consumption, and dependable performance. Their controlled motion ensures accurate locking alignment and reduces the possibility of mechanical failure. This makes the key access system more secure and efficient.

Working Methodology

The working methodology of the Smart Key Management System explains the complete operational flow of the system from user interaction to final output action. The proposed system is designed to provide secure, automated, and efficient access to physical keys through biometric authentication and embedded control mechanisms. Each operation follows a structured sequence, ensuring dependable performance and real-time response.

The overall operation of the system can be divided into three major stages: input acquisition, data processing with authentication, and output generation with access control. These stages function continuously in coordination to maintain uninterrupted service. By integrating sensing, processing, and actuation, the system reduces manual intervention while increasing security and reliability.

6.2 Overall Working Principle

The Smart Key Management System combines biometric identification with automated locking control to provide secure key access. When power is supplied, the ESP32 microcontroller initializes all connected devices, including the fingerprint sensor, LCD display, servo motor, LEDs, and buzzer. After initialization, the system enters standby mode and continuously waits for user input.

When a user requests access, they place a finger on the fingerprint sensor. The sensor captures the fingerprint image and converts it into a digital template. This template is transmitted to the ESP32, where it is compared with the stored fingerprint database.

If the fingerprint matches an authorized user, the authentication process is successful. The controller then activates the servo motor, which rotates to unlock the designated key compartment. Simultaneously, the LCD displays a message such as "Access Granted," and the green LED glows to indicate successful verification.

After a short delay, the servo motor returns to its original position, automatically locking the compartment again. This ensures that the key slot is not left open unnecessarily.

If the fingerprint does not match any stored record, the system immediately denies access. In this case, the red LED turns on, the buzzer sounds an alert, and the LCD displays "Access Denied." This prevents unauthorized individuals from obtaining access to stored keys.

The system continuously repeats this process, ensuring that it remains available at all times for secure and real-time operation.

6.3 Step-by-Step Working Process

The complete operation of the Smart Key Management System can be understood through the following sequence.

Initially, when the device is powered on, all hardware modules are initialized. The fingerprint sensor becomes active, the LCD displays the ready status, and the servo motor moves to the default locked position.

The system then enters standby mode and waits for the user to place a finger on the sensor. Once

detected, the sensor captures the fingerprint image and extracts identifying features. This processed biometric data is forwarded to the ESP32 controller. The controller compares the received fingerprint template with stored user templates in memory. If a valid match is found, the user is recognized as authorized. The LCD displays a success message, the green LED turns on, and the servo motor unlocks the assigned key slot.

The user is then allowed to access the key. After a predefined interval, the servo motor rotates back to the locked position automatically.

If no matching fingerprint is found, the user is treated as unauthorized. The LCD shows an access denial message, the red LED glows, and the buzzer is activated to indicate an invalid attempt.

This complete sequence is executed within a few seconds, making the system fast, efficient, and user-friendly.

Continuous Loop Operation

Continuous loop operation is one of the most important features of embedded systems. In the Smart Key Management System, the microcontroller program repeatedly executes instructions without interruption after power-up. This allows the system to remain active and ready for user interaction at all times.

In the ESP32 program, the main logic runs inside the loop() function. During each cycle, the controller checks whether a user has placed a finger on the sensor. If input is detected, the fingerprint is processed, authentication is performed, and outputs are generated according to the result.

After completing one cycle, the program returns to the beginning of the loop and starts again. This repeated execution allows the system to provide continuous monitoring, real-time response, and uninterrupted operation without requiring restart after every use.

Continuous loop processing is essential for automation systems because it ensures quick response and dependable service in dynamic environments.

Results

The Smart Key Management System was successfully designed and implemented using the ESP32 microcontroller, fingerprint sensor, servo motor, LCD display, buzzer, and LED indicators. The prototype was tested under multiple operating conditions to evaluate functionality, response time, and reliability.

During testing, the fingerprint sensor accurately identified authorized users whose templates were stored in memory. When a valid fingerprint was detected, the servo motor responded quickly by unlocking the assigned key slot. The green LED confirmed successful authentication, and the LCD displayed the corresponding message.

When an invalid fingerprint was presented, the system denied access instantly. The red LED turned on, the buzzer produced an alert sound, and the LCD displayed an access denial message.

These results confirm that the system performs the intended authentication and access functions successfully.

Fig 2 Final Output

Fig 3 ;Accessing through RFID Card

Discussion

The developed prototype demonstrates that biometric-based key management is significantly more secure and efficient than conventional manual methods. By eliminating manual registers and direct supervision, the system reduces human error and improves accountability.

One major advantage of the system is the ability to maintain records of access attempts, which supports monitoring and transparency. This feature is highly useful in workplaces where secure control of keys is required.

Some limitations were also identified. Sensor performance may be affected slightly by dust, moisture, or improper finger placement. In addition, stable power supply is important for consistent hardware performance. These issues can be minimized through proper maintenance and enclosure design.

Results and Performance Analysis

The system was tested for response time, recognition accuracy, and operational consistency. The fingerprint sensor showed high success rates in identifying enrolled users. The processing speed of the ESP32 ensured that authentication and access control occurred quickly.

The servo motor responded correctly during repeated lock and unlock cycles. Output devices provided clear status communication throughout operation.

The system successfully prevented unauthorized access during testing. Its performance remained stable over continuous operation, indicating suitability for real-world deployment in offices, laboratories, banks, and institutions.

Applications

The Smart Key Management System can be used in many sectors where secure handling of physical keys is important.

In offices and corporate buildings, it can control access to cabins, document rooms, and restricted departments. In educational institutions, it can manage laboratory, classroom, and equipment room keys.

Banks can use the system for locker keys, vault access, and secure record rooms. Industrial facilities may use it to control access to machinery rooms, tool stores, and maintenance areas.

Hospitals and laboratories can apply the system for medicine cabinets, diagnostic rooms, and restricted research sections. Hostels, apartments, and residential buildings may use it for room key management.

Hotels can manage master keys and staff access securely. Warehouses can control storage area keys, while libraries can protect restricted archives or special collections.

Government departments and defense organizations may also benefit from the system in high-security environments requiring controlled key usage.

Conclusion

The Smart Key Management System has been successfully designed and implemented as a secure, efficient, and automated solution for managing physical keys. By using fingerprint-based biometric authentication, the system ensures that only authorized users can access stored keys. This significantly improves security when compared with conventional manual methods.

The integration of ESP32, fingerprint sensor, servo motor, LCD display, buzzer, and LED indicators enables smooth and dependable operation. Real-time processing allows the system to remain continuously active and ready to respond immediately to user requests.

The automated locking and unlocking mechanism reduces manual effort and minimizes operational errors. At the same time, monitoring and tracking

capabilities improve accountability by maintaining control over key usage.

The project demonstrates how embedded systems and automation can solve practical security problems effectively. It is user-friendly, cost-effective, and suitable for deployment in offices, laboratories, banks, institutions, and storage facilities.

Future Scope

The Smart Key Management System has strong potential for future enhancement through modern technologies and intelligent automation.

One possible improvement is integration with the Internet of Things (IoT), allowing administrators to monitor and control the system remotely through mobile applications or web platforms. Users could check slot status, manage permissions, and receive updates from any location.

Cloud storage may be introduced for secure maintenance of user records and access logs. This would support centralized monitoring across multiple branches or departments.

Multi-factor authentication can further strengthen security by combining fingerprint verification with RFID cards, passwords, or PIN codes. Face recognition may also be added as an alternative biometric option.

A detailed logging system can record user name, access time, date, and activity history for advanced auditing purposes. Instant alerts through SMS, email, or mobile notifications may be sent during suspicious access attempts.

The hardware design can be upgraded from prototype form to a compact PCB-based commercial model. Battery backup or uninterrupted power systems can ensure operation during power failures.

In the future, the project can evolve into a fully intelligent, network-connected, and enterprise-level key management solution suitable for industries, institutions, smart buildings, and high-security environments.

References

[1] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*. USA: Springer, 2016.

[2] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in Embedded Systems: Design Challenges," *ACM Transactions on Embedded Computing Systems*, vol. 3, no. 3, pp. 461–491, 2017.

[3] Microchip Technology Inc., "RFID Based Access Control System," Application Note, USA, 2018.

[4] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards*. Wiley Publications, 2019.

[5] P. Kumar and M. Singh, "Design and Implementation of Smart Key Management System Using IoT," *International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. 6, pp. 234–239, 2020.

[6] Arduino, "Arduino Uno Rev3 Datasheet," Arduino Official Documentation, 2021.

[7] Espressif Systems, "ESP8266 Wi-Fi Module Datasheet," Espressif Inc., 2022.

[8] R. Sharma and S. Gupta, "IoT-Based Smart Locker System Using RFID and GSM," in *International Conference on Smart Systems and Inventive Technology*, India, 2022.

[9] NXP Semiconductors, "MFRC522 RFID Reader IC Datasheet," NXP, 2023.

[10] B. Patel and J. Desai, "Cloud-Based Smart Key Monitoring and Management System," *International Journal of Computer Applications*, vol. 185, no. 12, pp. 15–20, 2023.